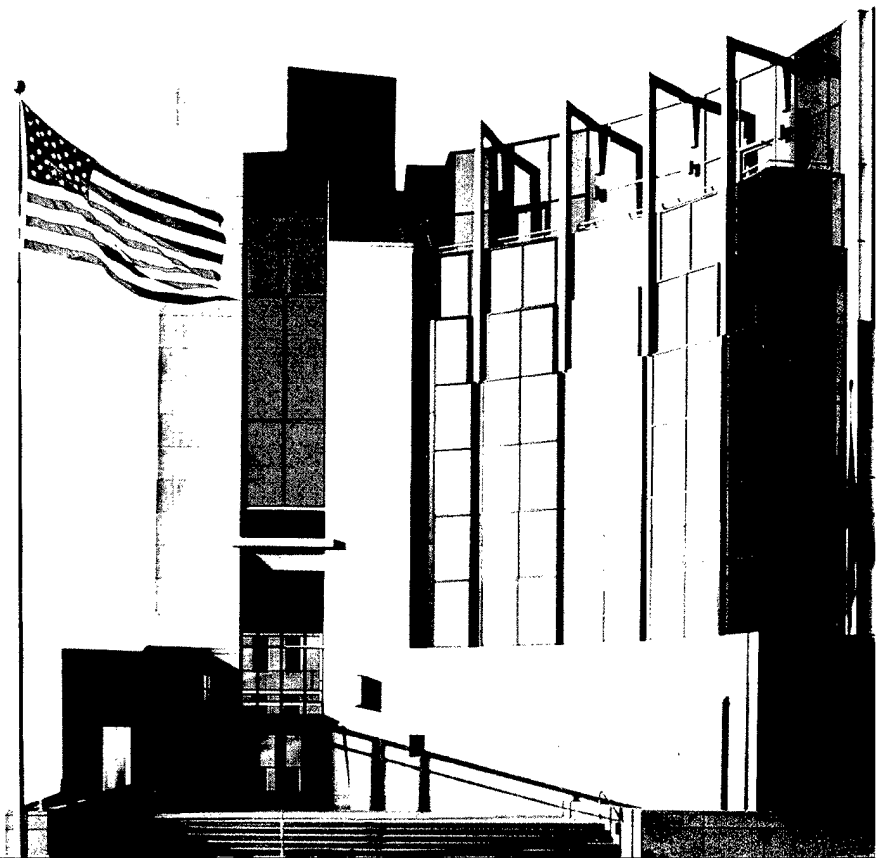
Carnegie Mellon
Software Engineering Institute

OCTAVE[SM] Catalog of Practices, Version 2.0

Christopher J. Alberts
Audrey J. Dorofee
Julia H. Allen

October 2001

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited



TECHNICAL REPORT
CMU/SEI-2001-TR-020
ESC-TR-2001-020

Carnegie Mellon
Software Engineering Institute
Pittsburgh, PA 15213-3890

OCTAVE[SM] Catalog of Practices, Version 2.0

CMU/SEI-2001-TR-020
ESC-TR-2001-020

Christopher J. Alberts
Audrey J. Dorofee
Julia H. Allen

October 2001

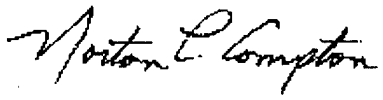
Networked Systems Survivability Program

This report was prepared for the

SEI Joint Program Office
HQ ESC/DIB
5 Eglin Street
Hanscom AFB, MA 01731-2116

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER



Norton L. Compton, Lt Col., USAF
SEI Joint Program Office

This work is sponsored by the U.S. Department of Defense and the U.S. Department of State. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 52.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

Table of Contents

List of Figures

Abstract

The Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE[SM]) Method enables organizations to identify the risks to their most important assets and build mitigation plans to address those risks. OCTAVE uses three "catalogs" of information to maintain modularity and keep the method separate from specific technologies. One of these catalogs is the catalog of good security practices. It provides the means to measure an organization's current security practices and to build a strategy for improving its practices to protect its critical assets.

The catalog of practices is divided into two types of practices – strategic and operational. The strategic practices focus on organizational issues at the policy level and provide good, general management practices. Operational practices focus on the technology-related issues dealing with how people use, interact with, and protect technology. This technical report describes how the catalog of practices is used in OCTAVE and describes the catalog in detail.

[SM] Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University.

1 Introduction

1.1 Purpose

This technical report describes the catalog of practices used with the Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE[SM]) Method. This catalog of good security practices is used with the self-directed information security risk evaluation

- to measure current organizational security practices
- to provide a basis for developing security improvement strategies and risk mitigation plans

Readers can view the catalog as a collection of what is currently known about good security practices (see the references for sources of the practices).

1.2 Background

Information systems are essential to most organizations today. However, many organizations form protection strategies by focusing solely on infrastructure weaknesses; they fail to establish the effect of those weaknesses on their most important information assets. This leads to a gap between the organization's operational and information technology (IT) requirements, placing the assets at risk. Current approaches to information security risk management tend to be incomplete. They fail to include all components of risk (assets, threats, and vulnerabilities). In addition, many organizations outsource information security risk evaluations. The resulting evaluation may not be adequate or address their perspectives. Self-directed assessments provide the context to understand the risks and to make informed decisions and trade-offs.

The first step in managing information security risk is to understand what your risks are. Once you have identified your risks, you can build mitigation plans to address those risks. OCTAVE enables you to do this by using an interdisciplinary analysis team of your own personnel.

OCTAVE is an approach to information security risk evaluations that is comprehensive, systematic, context driven, and self directed. The approach is embodied in a set of criteria that

[SM] Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University.

define the essential elements of an asset-driven information security risk evaluation. At this point, we have developed one method consistent with the OCTAVE criteria, called the OCTAVE Method [Alberts 01]. This method, designed with large organizations in mind, uses the catalog of practices defined in this report.

There can, however, be many implementations (or methods) consistent with the OCTAVE criteria (see Figure 1). Any one of these methods could use the catalog of practices or a variation of this catalog. For example, the criteria would be implemented differently in a very large organization than in a very small one, but both could use the same catalog of practices. Also, a catalog of practices specific to a particular domain (e.g., the financial community) could be used. The catalog of practices in this report can be considered a general, broadly applicable catalog.

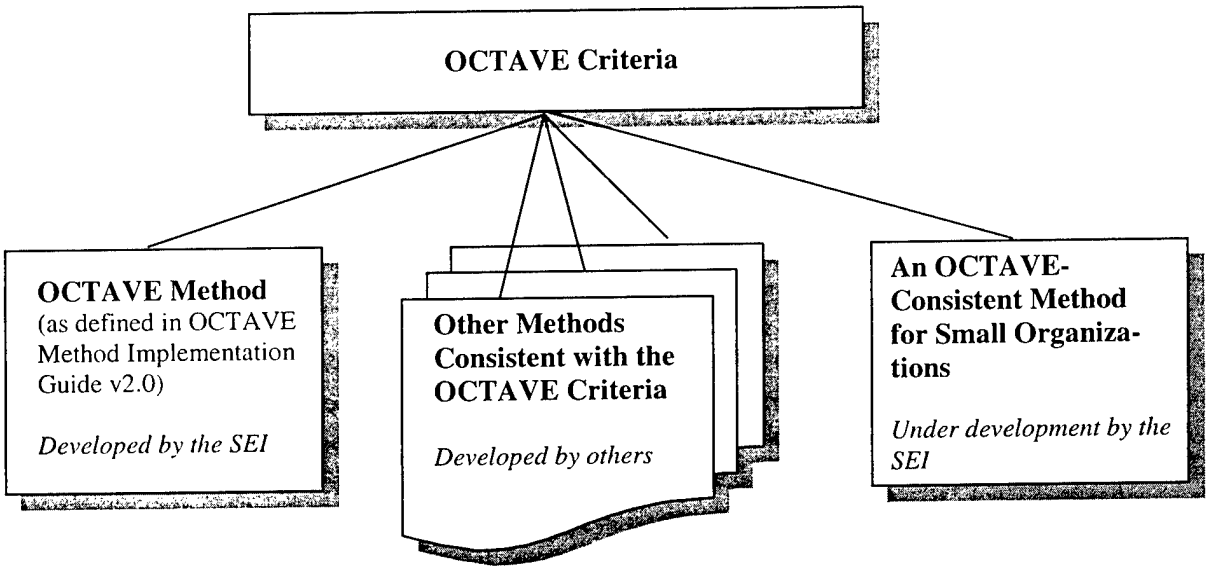


Figure 1: Multiple Methods Consistent with the OCTAVE Criteria

1.3 OCTAVE Catalog of Practices

The catalog of practices used in the OCTAVE Method and defined here comprises a collection of good strategic and operational security practices. An organization that is conducting an information security risk evaluation measures itself against the catalog of practices to determine what it is currently doing well with respect to security (its current protection strategy practices) and what it is not doing well (its organizational vulnerabilities). It is also used as a basis for defining security improvement strategies and risk mitigation plans.

The next section describes the OCTAVE Method and details how the catalog of practices is used in the method.

2 Overview of the OCTAVE Method

2.1 Three Phases of OCTAVE

The OCTAVE Method uses a three-phase approach (see Figure 2) to examine organizational and technology issues, assembling a comprehensive picture of the organization's information security needs. Each phase consists of several processes. These phases and their processes are described below.

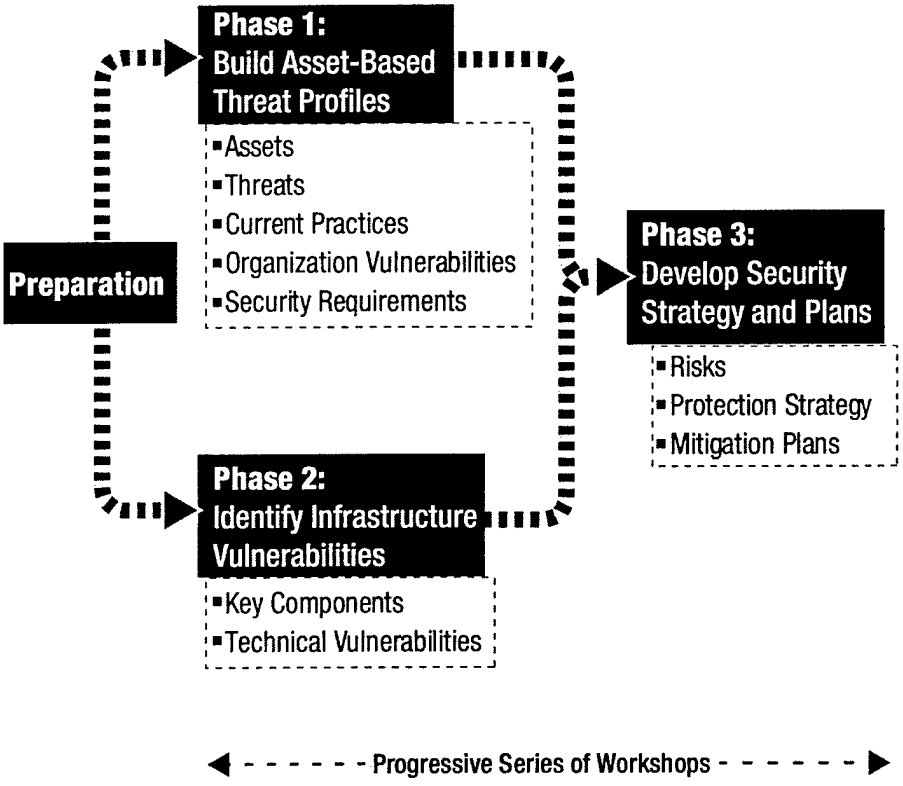


Figure 2: The OCTAVE Method

2.1.1 Phase 1: Build Asset-Based Threat Profiles

This phase is an organizational evaluation. The analysis team determines which assets are most important to the organization (critical assets) and identifies what is currently being done

to protect those assets. Surveys based on the catalog of practices are used to elicit the information from the organization's personnel about what is being done well with respect to security practices. These surveys are provided in the appendix. The processes of Phase 1 are

- Process 1: Identify Senior Management Knowledge – Selected senior managers identify important assets, perceived threats, security requirements, current security practices, and organizational vulnerabilities.
- Process 2: Identify Operational Area Management Knowledge – Selected operational area managers identify important assets, perceived threats, security requirements, current security practices, and organizational vulnerabilities.
- Process 3: Identify Staff Knowledge – Selected general and IT staff members identify important assets, perceived threats, security requirements, current security practices, and organizational vulnerabilities.
- Process 4: Create Threat Profiles – The analysis team analyzes the information from Processes 1 through 3, selects critical assets, refines the security requirements associated with those assets, and identifies threats to the critical assets, creating threat profiles.

2.1.2 Phase 2: Identify Infrastructure Vulnerabilities

This phase is an evaluation of the information infrastructure. The analysis team examines key operational components for weaknesses (technology vulnerabilities) that can lead to unauthorized action against critical assets. The processes of Phase 2 are

- Process 5: Identify Key Components – The analysis team identifies key information technology systems and components for each critical asset. Specific instances are then selected for evaluation.
- Process 6: Evaluate Selected Components – The analysis team examines the key systems and components for technology weaknesses. Vulnerability tools (software, checklists, scripts) are used. The results are examined and summarized, looking for the relevance to the critical assets and their threat profiles.

2.1.3 Phase 3: Develop Security Strategy and Plans

During this part of the evaluation, the analysis team identifies risks to the organization's critical assets and decides whether and how to address those risks. The processes of Phase 3 are

- Process 7: Conduct Risk Analysis – The analysis team identifies the impact of threats to critical assets to define risks, develops criteria to evaluate those risks, and evaluates the risk impacts based on those criteria. This produces a risk profile for each critical asset.
- Process 8: Develop Protection Strategy – The analysis team creates a protection strategy for the organization and mitigation plans for the critical assets, based upon an analysis of the information gathered. Senior managers then review, refine, and approve the strategy and plans.

2.2 How the Catalog of Practices Is Used

The catalog of practices is used primarily in two places in the OCTAVE Method. In Phase 1, the catalog is used during Processes 1-3. These processes are also known as knowledge elicitation workshops, where participants contribute their knowledge and understanding about security-related issues. One of the activities in Processes 1-3 is to determine the current security practices and organizational vulnerabilities from the perspectives of the participants in the workshops.

Participants in a knowledge elicitation workshop complete a survey based on the catalog of practices and then participate in a discussion centered around the practice areas from the surveys. During these discussions, participants identify specific practices that are currently working well in the organization (security practices). They also identify specific weaknesses with current security practices (organizational vulnerabilities) in the organization.

The catalog of practices is also used is during Process 8 of the OCTAVE Method, when the protection strategy and risk mitigation plans are developed. The areas highlighted in the catalog of practices are used to frame the protection strategy. In addition, the practices from the catalog of practices are used as a reference when the analysis team selects actions for the risk mitigation plans. Details of how the catalog of practices is used in the OCTAVE Method can be found in the *OCTAVE Method Implementation Guide v 2.0* [Alberts 01].

In the remainder of this document, we present the OCTAVE catalog of practices.

3 Catalog of Practices

This section focuses on the catalog of practices used in the OCTAVE Method. The surveys completed during the knowledge elicitation workshops are developed from the catalog of practices by selecting practices that are more than likely to be used by (or should be applicable at) a certain level of personnel. For example, senior managers are more likely to know if corporate strategy and plans include or address security issues, while information technology (IT) personnel are more likely to be familiar with particular aspects of managing technological vulnerabilities and firewalls.

The catalog of practices is divided into two types of practices – strategic and operational. Strategic practices focus on organizational issues at the policy level and provide good, general management practices. Strategic practices address business-related issues as well as issues that require organization-wide plans and participation. Operational practices, on the other hand, focus on technology-related issues dealing with how people use, interact with, and protect technology. Since strategic practices are based on good management practice, they should be fairly stable over time. Operational practices are more subject to changes as technology advances and new or updated practices arise to deal with those changes.

The catalog of practices is a general catalog; it is not specific to any domain, organization, or set of regulations. It can be modified to suit a particular domain's standard of due care or set of regulations (e.g., the medical community and Health Insurance Portability and Accountability Act [HIPAA] security regulations, the financial community and Gramm-Leach-Bliley regulations). It can also be extended to add organization-specific standards, or it can be modified to reflect the terminology of a specific domain.

Figure 3 on the next page depicts the structure of the catalog of practices; the details of the specific practices can be found on the following pages. This catalog was developed using several sources that describe information security practices [BSI 95, Treasury 01, HHS 98, Swanson 96]. In addition to these security-related references, we also used our experience developing, delivering, and analyzing the results of the Information Security Evaluation (ISE), a vulnerability assessment technique developed by the Software Engineering Institute and delivered to a variety of organization over the past six years. Specific technical practices can be found in resources such as the *CERT Guide to System and Network Security* [Allen 01].

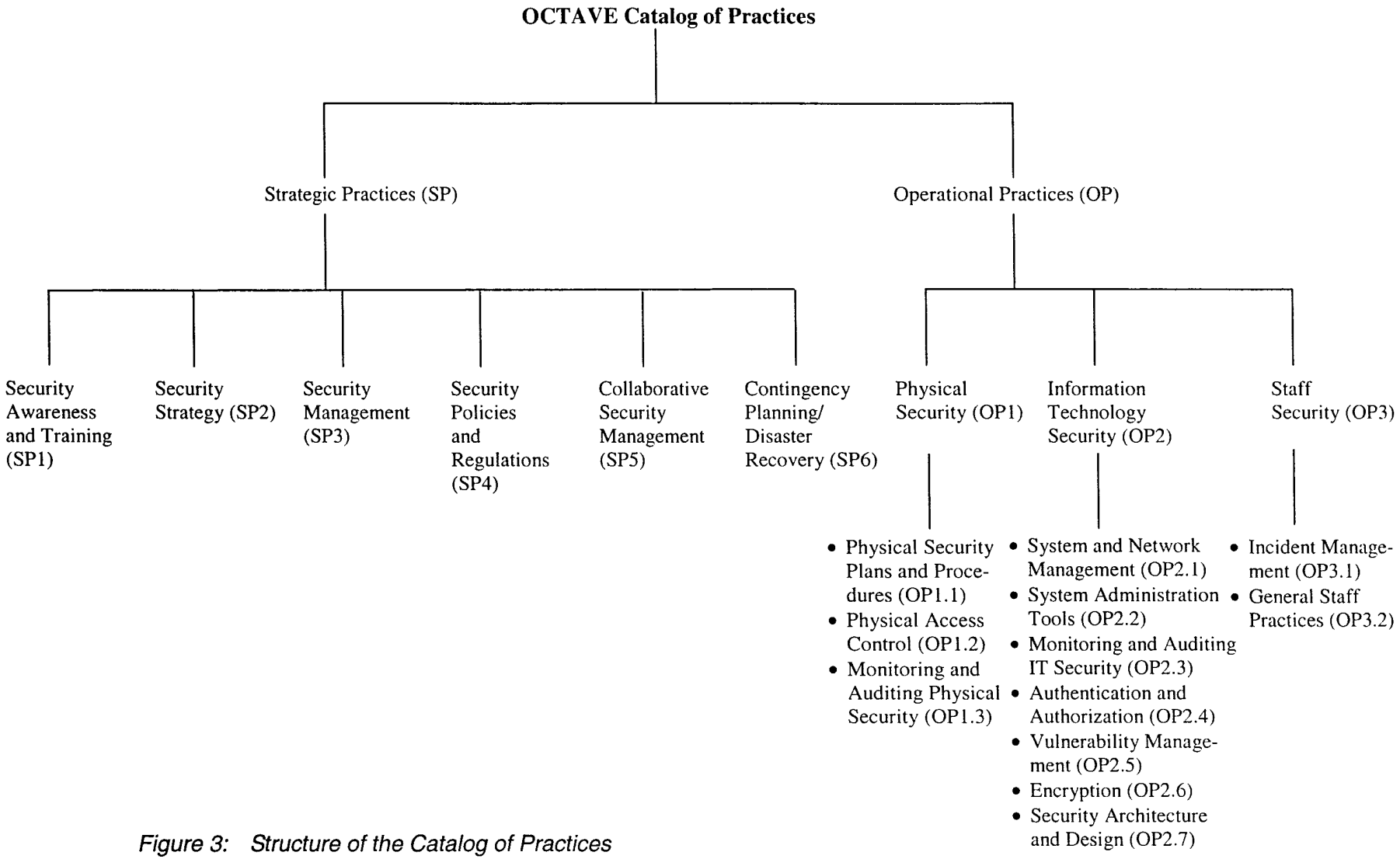


Figure 3: Structure of the Catalog of Practices

Strategic Practices Security Awareness and Training (SP1)	
SP1.1	Staff members understand their security roles and responsibilities. This is documented and verified.
SP1.2	There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified.
SP1.3	Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. Training includes these topics: • security strategies, goals, and objectives • security regulations, polices, and procedures • policies and procedures for working with third parties • contingency and disaster recovery plans • physical security requirements • users' perspective on – system and network management – system administration tools – monitoring and auditing for physical and information technology security – authentication and authorization – vulnerability management – encryption – architecture and design • incident management • general staff practices • enforcement, sanctions, and disciplinary actions for security violations • how to properly access sensitive information or work in areas where sensitive information is accessible • termination policies and procedures relative to security

Strategic Practices Security Strategy (SP2)	
SP2.1	The organization's business strategies routinely incorporate security considerations.
SP2.2	Security strategies and policies take into consideration the organization's business strategies and goals.
SP2.3	Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization.

Strategic Practices Security Management (SP3)	
SP3.1	Management allocates sufficient funds and resources to information security activities.
SP3.2	Security roles and responsibilities are defined for all staff in the organization.
SP3.3	The organization's hiring and termination practices for staff take information security issues into account.
SP3.4	The required levels of information security and how they are applied to individuals and groups are documented and enforced.
SP3.5	The organization manages information security risks, including • assessing risks to information security both periodically and in response to major changes in technology, internal/external threats, or the organization's systems and operations • taking steps to mitigate risks to an acceptable level • maintaining an acceptable level of risk • using information security risk assessments to help select cost-effective security/control measures, balancing implementation costs against potential losses
SP3.6	Management receives and acts upon routine reports summarizing the results of • review of system logs • review of audit trails • technology vulnerability assessments • security incidents and the responses to them • risk assessments • physical security reviews • security improvement plans and recommendations

Strategic Practices Security Policies and Regulations (SP4)	
SP4.1	The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. These policies address key security topic areas, including • security strategy and management • security risk management • physical security • system and network management • system administration tools • monitoring and auditing • authentication and authorization • vulnerability management • encryption • security architecture and design • incident management • staff security practices • applicable laws and regulations • awareness and training • collaborative information security • contingency planning and disaster recovery
SP4.2	There is a documented process for management of security policies, including • creation • administration (including periodic reviews and updates) • communication
SP4.3	The organization has a documented process for periodic evaluation (technical and non-technical) of compliance with information security policies, applicable laws and regulations, and insurance requirements.
SP4.4	The organization has a documented process to ensure compliance with information security policies, applicable laws and regulations, and insurance requirements.
SP4.5	The organization uniformly enforces its security policies.
SP4.6	Testing and revision of security policies and procedures is restricted to authorized personnel.

Strategic Practices Collaborative Security Management (SP5)	
SP5.1	The organization has documented, monitored, and enforced procedures for protecting its information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners).
SP5.2	The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements.
SP5.3	The organization documents, monitors, and enforces protection strategies for information belonging to external organizations that is accessed from its own infrastructure components or is used by its own personnel.
SP5.4	The organization provides and verifies awareness and training on applicable external organizations' security polices and procedures for personnel who are involved with those external organizations.
SP5.5	There are documented procedures for terminated external personnel specifying appropriate security measures for ending their access. These procedures are communicated and coordinated with the external organization.

Strategic Practices Contingency Planning/Disaster Recovery (SP6)	
SP6.1	An analysis of operations, applications, and data criticality has been performed.
SP6.2	The organization has documented • business continuity or emergency operation plans • disaster recovery plan(s) • contingency plan(s) for responding to emergencies
SP6.3	The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.
SP6.4	The contingency, disaster recovery, and business continuity plans are periodically reviewed, tested, and revised.
SP6.5	All staff are • aware of the contingency, disaster recovery, and business continuity plans • understand and are able to carry out their responsibilities

Operational Practices Physical Security (OP1) Physical Security Plans and Procedures (OP1.1)	
OP1.1.1	There are documented facility security plan(s) for safeguarding the premises, buildings, and any restricted areas.
OP1.1.2	These plans are periodically reviewed, tested, and updated.
OP1.1.3	Physical security procedures and mechanisms are routinely tested and revised.
OP1.1.4	There are documented policies and procedures for managing visitors, including • sign in • escort • access logs • reception and hosting
OP1.1.5	There are documented policies and procedures for physical control of hardware and software, including • workstations, laptops, modems, wireless components, and all other components used to access information • access, storage, and retrieval of data backups • storage of sensitive information on physical and electronic media • disposal of sensitive information or the media on which it is stored • reuse and recycling of paper and electronic media

Operational Practices Physical Security (OP1) Physical Access Control (OP1.2)	
OP1.2.1	There are documented policies and procedures for individual and group access covering • the rules for granting the appropriate level of physical access • the rules for setting an initial right of access • modifying the right of access • terminating the right of access • periodically reviewing and verifying the rights of access
OP1.2.2	There are documented policies, procedures, and mechanisms for controlling physical access to defined entities. This includes • work areas • hardware (computers, communication devices, etc.) and software media
OP1.2.3	There are documented procedures for verifying access authorization prior to granting physical access.
OP1.2.4	Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.

Operational Practices Physical Security (OP1) Monitoring and Auditing Physical Security (OP1.3)	
OP1.3.1	Maintenance records are kept to document the repairs and modifications of a facility's physical components.
OP1.3.2	An individual's or group's actions, with respect to all physically controlled media, can be accounted for.
OP1.3.3	Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed.

Operational Practices Information Technology Security (OP2) System and Network Management (OP2.1)	
OP2.1.1	There are documented security plan(s) for safeguarding the systems and networks.
OP2.1.2	Security plan(s) are periodically reviewed, tested, and updated.
OP2.1.3	Sensitive information is protected by secure storage, such as • defined chains of custody • backups stored off site • removable storage media • discard process for sensitive information or its storage media
OP2.1.4	The integrity of installed software is regularly verified.
OP2.1.5	All systems are up to date with respect to revisions, patches, and recommendations in security advisories.
OP2.1.6	There is a documented data backup plan that • is routinely updated • is periodically tested • calls for regularly scheduled backups of both software and data • requires periodic testing and verification of the ability to restore from backups
OP2.1.7	All staff understand and are able to carry out their responsibilities under the backup plans.
OP2.1.8	Changes to IT hardware and software are planned, controlled, and documented.
OP2.1.9	IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. • Unique user identification is required for all information system users, including third-party users. • Default accounts and default passwords have been removed from systems.
OP2.1.10	Only necessary services are running on systems – all unnecessary services have been removed.

Operational Practices Information Technology Security (OP2) System Administration Tools (OP2.2)	
OP2.2.1	New security tools, procedures, and mechanisms are routinely reviewed for applicability in meeting the organization's security strategies.
OP2.2.2	Tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced. Examples are • data integrity checkers • cryptographic tools • vulnerability scanners • password quality-checking tools • virus scanners • process management tools • intrusion detection systems • secure remote administrations • network service tools • traffic analyzers • incident response tools • forensic tools for data analysis

Operational Practices Information Technology Security (OP2) Monitoring and Auditing IT Security (OP2.3)	
OP2.3.1	System and network monitoring and auditing tools are routinely used by the organization. • Activity is monitored by the IT staff. • System and network activity is logged/recorded. • Logs are reviewed on a regular basis. • Unusual activity is dealt with according to the appropriate policy or procedure. • Tools are periodically reviewed and updated.
OP2.3.2	Firewall and other security components are periodically audited for compliance with policy.

Operational Practices Information Technology Security (OP2) Authentication and Authorization (OP2.4)	
OP2.4.1	Appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to • information • systems utilities • program source code • sensitive systems • specific applications and services • network connections within the organization • network connections from outside the organization
OP2.4.2	There are documented information-use policies and procedures for individual and group access to • establish the rules for granting the appropriate level of access • establish an initial right of access • modify the right of access • terminate the right of access • periodically review and verify the rights of access
OP2.4.3	Access control methods/mechanisms restrict access to resources according to the access rights determined by policies and procedures.
OP2.4.4	Access control methods/mechanisms are periodically reviewed and verified.
OP2.4.5	Methods or mechanisms are provided to ensure that sensitive information has not been accessed, altered, or destroyed in an unauthorized manner.
OP2.4.6	Authentication mechanisms are used to protect availability, integrity, and confidentiality of sensitive information. Examples are • digital signatures • biometrics

Operational Practices Information Technology Security (OP2) Vulnerability Management (OP2.5)	
OP2.5.1	There is a documented set of procedures for managing vulnerabilities, including • selecting vulnerability evaluation tools, checklists, and scripts • keeping up to date with known vulnerability types and attack methods • reviewing sources of information on vulnerability announcements, security alerts, and notices • identifying infrastructure components to be evaluated • scheduling of vulnerability evaluations • interpreting and responding to the results • maintaining secure storage and disposition of vulnerability data
OP2.5.2	Vulnerability management procedures are followed and are periodically reviewed and updated.
OP2.5.3	Technology vulnerability assessments are performed on a periodic basis, and vulnerabilities are addressed when they are identified.

Operational Practices Information Technology Security (OP2) Encryption (OP2.6)	
OP2.6.1	Appropriate security controls are used to protect sensitive information while in storage and during transmission, including • data encryption during transmission • data encryption when writing to disk • use of public key infrastructure • virtual private network technology • encryption for all Internet-based transmission
OP2.6.2	Encrypted protocols are used when remotely managing systems, routers, and firewalls.
OP2.6.3	Encryption controls and protocols are routinely reviewed, verified, and revised.

Operational Practices Information Technology Security (OP2) Security Architecture and Design (OP2.7)	
OP2.7.1	System architecture and design for new and revised systems include considerations for • security strategies, policies, and procedures • history of security compromises • results of security risk assessments
OP2.7.2	The organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.

Operational Practices Staff Security (OP3) Incident Management (OP3.1)	
OP3.1.1	Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations, including • network-based incidents • physical access incidents • social engineering incidents
OP3.1.2	Incident management procedures are periodically tested, verified, and updated.
OP3.1.3	There are documented policies and procedures for working with law enforcement agencies.

Operational Practices Staff Security (OP3) General Staff Practices (OP3.2)	
OP3.2.1	Staff members follow good security practice, such as • securing information for which they are responsible • not divulging sensitive information to others (resistance to social engineering) • having adequate ability to use information technology hardware and software • using good password practices • understanding and following security policies and regulations • recognizing and reporting incidents
OP3.2.2	All staff at all levels of responsibility implement their assigned roles and responsibility for information security.
OP3.2.3	There are documented procedures for authorizing and overseeing those who work with sensitive information or who work in locations where the information resides. This includes • employees • contractors, partners, collaborators, and personnel from third-party organizations • systems maintenance personnel • facilities maintenance personnel

4 Summary

The OCTAVE Method is a security risk evaluation focused on the organization's assets and the risks to those assets. It is comprehensive, systematic, context driven, and self directed. It enables people at all levels of an organization to work together to identify and understand their security risks and to make the right decisions about mitigation and protection.

The catalog of practices is an artifact of the OCTAVE Method. It is used during Processes 1-3 (the knowledge elicitation workshop) to measure organizational practices. Workshop participants determine which specific practices are currently working well in the organization (security practices) as well as specific weaknesses with current security practices (organizational vulnerabilities). The catalog is also used during Process 8 as a framework for the organization's protection strategy and as a reference when the analysis team selects actions for the risk mitigation plans.

Appendix: Surveys

This appendix lists the surveys used during Processes 1 through 3 to elicit information about current security practices from different levels of the organization. Four surveys are provided for

- senior managers
- operational area managers
- general staff
- information technology staff

These surveys are derived from the catalog of practices by selecting a set of practices relevant to the specific organizational level. For example, strategic practices are in the management-oriented survey, while detailed technical practices are in the information technology staff survey.

Senior Management Survey			
Practice	**Is this practice used by your organization?**		
Security Awareness and Training			
Staff members understand their security roles and responsibilities. This is documented and verified.	Yes	No	Don't Know
There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified.	Yes	No	Don't Know
Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified.	Yes	No	Don't Know
Security Strategy			
The organization's business strategies routinely incorporate security considerations.	Yes	No	Don't Know
Security strategies and policies take into consideration the organization's business strategies and goals.	Yes	No	Don't Know
Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization.	Yes	No	Don't Know
Security Management			
Management allocates sufficient funds and resources to information security activities.	Yes	No	Don't Know
Security roles and responsibilities are defined for all staff in the organization.	Yes	No	Don't Know
The organization's hiring and termination practices for staff take information security issues into account.	Yes	No	Don't Know

Senior Management Survey (cont.)			
Practice	**Is this practice used by your organization?**		
Security Management (cont.)			
The organization manages information security risks, including • assessing risks to information security • taking steps to mitigate information security risks	Yes	No	Don't Know
Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments).	Yes	No	Don't Know
Security Policies and Regulations			
The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated.	Yes	No	Don't Know
There is a documented process for management of security policies, including • creation • administration (including periodic reviews and updates) • communication	Yes	No	Don't Know
The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements.	Yes	No	Don't Know
The organization uniformly enforces its security policies.	Yes	No	Don't Know

Senior Management Survey (cont.)			
Practice	**Is this practice used by your organization?**		
Collaborative Security Management			
The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including • protecting information belonging to other organizations • understanding the security polices and procedures of external organizations • ending access to information by terminated external personnel	Yes	No	Don't Know
The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements.	Yes	No	Don't Know
Contingency Planning/Disaster Recovery			
An analysis of operations, applications, and data criticality has been performed.	Yes	No	Don't Know
The organization has documented, reviewed, and tested • business continuity or emergency operation plans • disaster recovery plan(s) • contingency plan(s) for responding to emergencies	Yes	No	Don't Know
The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.	Yes	No	Don't Know
All staff are • aware of the contingency, disaster recovery, and business continuity plans • understand and are able to carry out their responsibilities	Yes	No	Don't Know

Senior Management Survey (cont.)			
Practice	**Is this practice used by your organization?**		
Physical Security Plans and Procedures			
Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested.	Yes	No	Don't Know
There are documented policies and procedures for managing visitors.	Yes	No	Don't Know
There are documented policies and procedures for physical control of hardware and software.	Yes	No	Don't Know
Physical Access Control			
There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media.	Yes	No	Don't Know
Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.	Yes	No	Don't Know
System and Network Management			
There are documented and tested security plan(s) for safeguarding the systems and networks.	Yes	No	Don't Know
There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans.	Yes	No	Don't Know
Authentication and Authorization			
There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups.	Yes	No	Don't Know

Senior Management Survey (cont.)			
Practice	**Is this practice used by your organization?**		
Incident Management			
Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations.	Yes	No	Don't Know
Incident management procedures are periodically tested, verified, and updated.	Yes	No	Don't Know
There are documented policies and procedures for working with law enforcement agencies.	Yes	No	Don't Know
General Staff Practices			
Staff members follow good security practice, such as • securing information for which they are responsible • not divulging sensitive information to others (resistance to social engineering) • having adequate ability to use information technology hardware and software • using good password practices • understanding and following security policies and regulations • recognizing and reporting incidents	Yes	No	Don't Know
All staff at all levels of responsibility implement their assigned roles and responsibility for information security.	Yes	No	Don't Know
There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides.	Yes	No	Don't Know

Operational Area Management Survey			
Practice	**Is this practice used by your organization?**		
Security Awareness and Training			
Staff members understand their security roles and responsibilities. This is documented and verified.	Yes	No	Don't Know
There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified.	Yes	No	Don't Know
Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified.	Yes	No	Don't Know
Security Strategy			
The organization's business strategies routinely incorporate security considerations.	Yes	No	Don't Know
Security strategies and policies take into consideration the organization's business strategies and goals.	Yes	No	Don't Know
Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization.	Yes	No	Don't Know
Security Management			
Management allocates sufficient funds and resources to information security activities.	Yes	No	Don't Know
Security roles and responsibilities are defined for all staff in the organization.	Yes	No	Don't Know
The organization's hiring and termination practices for staff take information security issues into account.	Yes	No	Don't Know

Operational Area Management Survey (cont.)	
Practice	**Is this practice used by your organization?**
Security Management (cont.)	
The organization manages information security risks, including • assessing risks to information security • taking steps to mitigate information security risks	Yes No Don't Know
Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments).	Yes No Don't Know
Security Policies and Regulations	
The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated.	Yes No Don't Know
There is a documented process for management of security policies, including • creation • administration (including periodic reviews and updates) • communication	Yes No Don't Know
The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements.	Yes No Don't Know
The organization uniformly enforces its security policies.	Yes No Don't Know

Operational Area Management Survey (cont.)	
Practice	**Is this practice used by your organization?**
Collaborative Security Management	
The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including • protecting information belonging to other organizations • understanding the security polices and procedures of external organizations • ending access to information by terminated external personnel	Yes No Don't Know
The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements.	Yes No Don't Know
Contingency Planning/Disaster Recovery	
An analysis of operations, applications, and data criticality has been performed.	Yes No Don't Know
The organization has documented, reviewed, and tested • business continuity or emergency operation plans • disaster recovery plan(s) • contingency plan(s) for responding to emergencies	Yes No Don't Know
The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.	Yes No Don't Know
All staff are • aware of the contingency, disaster recovery, and business continuity plans • understand and are able to carry out their responsibilities	Yes No Don't Know

Operational Area Management Survey (cont.)			
Practice	**Is this practice used by your organization?**		
Physical Security Plans and Procedures			
Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested.	Yes	No	Don't Know
There are documented policies and procedures for managing visitors.	Yes	No	Don't Know
There are documented policies and procedures for physical control of hardware and software.	Yes	No	Don't Know
Physical Access Control			
There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media.	Yes	No	Don't Know
Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.	Yes	No	Don't Know
Monitoring and Auditing Physical Security			
Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed.	Yes	No	Don't Know
System and Network Management			
There are documented and tested security plan(s) for safeguarding the systems and networks.	Yes	No	Don't Know
There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans.	Yes	No	Don't Know

Operational Area Management Survey (cont.)			
Practice	**Is this practice used by your organization?**		
Authentication and Authorization			
There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups.	Yes	No	Don't Know
Incident Management			
Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations.	Yes	No	Don't Know
Incident management procedures are periodically tested, verified, and updated.	Yes	No	Don't Know
There are documented policies and procedures for working with law enforcement agencies.	Yes	No	Don't Know
General Staff Practices			
Staff members follow good security practice, such as • securing information for which they are responsible • not divulging sensitive information to others (resistance to social engineering) • having adequate ability to use information technology hardware and software • using good password practices • understanding and following security policies and regulations • recognizing and reporting incidents	Yes	No	Don't Know
All staff at all levels of responsibility implement their assigned roles and responsibility for information security.	Yes	No	Don't Know
There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides.	Yes	No	Don't Know

Staff Survey			
Practice	**Is this practice used by your organization?**		
Security Awareness and Training			
Staff members understand their security roles and responsibilities. This is documented and verified.	Yes	No	Don't Know
There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified.	Yes	No	Don't Know
Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified.	Yes	No	Don't Know
Security Management			
Management allocates sufficient funds and resources to information security activities.	Yes	No	Don't Know
Security roles and responsibilities are defined for all staff in the organization.	Yes	No	Don't Know
The organization's hiring and termination practices for staff take information security issues into account.	Yes	No	Don't Know
The organization manages information security risks, including • assessing risks to information security • taking steps to mitigate information security risks	Yes	No	Don't Know

Staff Survey (cont.)	
Practice	**Is this practice used by your organization?**
Security Policies and Regulations	
The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated.	Yes No Don't Know
There is a documented process for management of security policies, including • creation • administration (including periodic reviews and updates) • communication	Yes No Don't Know
The organization uniformly enforces its security policies.	Yes No Don't Know
Collaborative Security Management	
The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including • protecting information belonging to other organizations • understanding the security polices and procedures of external organizations • ending access to information by terminated external personnel	Yes No Don't Know
Contingency Planning/Disaster Recovery	
All staff are • aware of the contingency, disaster recovery, and business continuity plans • understand and are able to carry out their responsibilities	Yes No Don't Know

Staff Survey (cont.)			
Practice	**Is this practice used by your organization?**		
Physical Security Plans and Procedures			
Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested.	Yes	No	Don't Know
There are documented policies and procedures for managing visitors.	Yes	No	Don't Know
There are documented policies and procedures for physical control of hardware and software.	Yes	No	Don't Know
Physical Access Control			
There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media.	Yes	No	Don't Know
Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.	Yes	No	Don't Know
System and Network Management			
There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans.	Yes	No	Don't Know
Incident Management			
Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations.	Yes	No	Don't Know
Incident management procedures are periodically tested, verified, and updated.	Yes	No	Don't Know
There are documented policies and procedures for working with law enforcement agencies.	Yes	No	Don't Know

Staff Survey (cont.)			
Practice	**Is this practice used by your organization?**		
General Staff Practices			
Staff members follow good security practice, such as • securing information for which they are responsible • not divulging sensitive information to others (resistance to social engineering) • having adequate ability to use information technology hardware and software • using good password practices • understanding and following security policies and regulations • recognizing and reporting incidents	Yes	No	Don't Know
All staff at all levels of responsibility implement their assigned roles and responsibility for information security.	Yes	No	Don't Know
There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides.	Yes	No	Don't Know

IT Staff Survey			
Practice	**Is this practice used by your organization?**		
Security Awareness and Training			
Staff members understand their security roles and responsibilities. This is documented and verified.	Yes	No	Don't Know
There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified.	Yes	No	Don't Know
Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified.	Yes	No	Don't Know
Security Strategy			
The organization's business strategies routinely incorporate security considerations.	Yes	No	Don't Know
Security strategies and policies take into consideration the organization's business strategies and goals.	Yes	No	Don't Know
Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization.	Yes	No	Don't Know
Security Management			
Management allocates sufficient funds and resources to information security activities.	Yes	No	Don't Know
Security roles and responsibilities are defined for all staff in the organization.	Yes	No	Don't Know

IT Staff Survey (cont.)			
Practice	**Is this practice used by your organization?**		
Security Management (cont.)			
The organization's hiring and termination practices for staff take information security issues into account.	Yes	No	Don't Know
The organization manages information security risks, including • assessing risks to information security • taking steps to mitigate information security risks	Yes	No	Don't Know
Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments).	Yes	No	Don't Know
Security Policies and Regulations			
The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated.	Yes	No	Don't Know
There is a documented process for management of security policies, including • creation • administration (including periodic reviews and updates) • communication	Yes	No	Don't Know
The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements.	Yes	No	Don't Know
The organization uniformly enforces its security policies.	Yes	No	Don't Know

IT Staff Survey (cont.)			
Practice	**Is this practice used by your organization?**		
Collaborative Security Management			
The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including • protecting information belonging to other organizations • understanding the security polices and procedures of external organizations • ending access to information by terminated external personnel	Yes	No	Don't Know
The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements.	Yes	No	Don't Know
Contingency Planning/Disaster Recovery			
An analysis of operations, applications, and data criticality has been performed.	Yes	No	Don't Know
The organization has documented, reviewed, and tested • business continuity or emergency operation plans • disaster recovery plan(s) • contingency plan(s) for responding to emergencies	Yes	No	Don't Know
The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.	Yes	No	Don't Know
All staff are • aware of the contingency, disaster recovery, and business continuity plans • understand and are able to carry out their responsibilities	Yes	No	Don't Know

IT Staff Survey (cont.)			
Practice	**Is this practice used by your organization?**		
Physical Security Plans and Procedures			
Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested.	Yes	No	Don't Know
There are documented policies and procedures for managing visitors.	Yes	No	Don't Know
There are documented policies and procedures for physical control of hardware and software.	Yes	No	Don't Know
Physical Access Control			
There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media.	Yes	No	Don't Know
Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.	Yes	No	Don't Know
Monitoring and Auditing Physical Security			
Maintenance records are kept to document the repairs and modifications of a facility's physical components.	Yes	No	Don't Know
An individual's or group's actions, with respect to all physically controlled media, can be accounted for.	Yes	No	Don't Know
Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed.	Yes	No	Don't Know

IT Staff Survey (cont.)			
Practice	**Is this practice used by your organization?**		
System and Network Management			
There are documented and tested security plan(s) for safeguarding the systems and networks.	Yes	No	Don't Know
Sensitive information is protected by secure storage (e.g., backups stored off site, discard process for sensitive information).	Yes	No	Don't Know
The integrity of installed software is regularly verified.	Yes	No	Don't Know
All systems are up to date and with respect to revisions, patches, and recommendations in security advisories.	Yes	No	Don't Know
There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans.	Yes	No	Don't Know
Changes to IT hardware and software are planned, controlled, and documented.	Yes	No	Don't Know
IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. • Unique user identification is required for all information system users, including third-party users. • Default accounts and default passwords have been removed from systems.	Yes	No	Don't Know
Only necessary services are running on systems – all unnecessary services have been removed.	Yes	No	Don't Know

IT Staff Survey (cont.)			
Practice	**Is this practice used by your organization?**		
System Administration Tools			
Tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced.	Yes	No	Don't Know
Monitoring and Auditing IT Security			
System and network monitoring and auditing tools are routinely used by the organization. Unusual activity is dealt with according to the appropriate policy or procedure.	Yes	No	Don't Know
Firewall and other security components are periodically audited for compliance with policy.	Yes	No	Don't Know
Authentication and Authorization			
Appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, sensitive systems, specific applications and services, and network connections.	Yes	No	Don't Know
There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups.	Yes	No	Don't Know
Methods or mechanisms are provided to ensure that sensitive information has not been accessed, altered, or destroyed in an unauthorized manner. Methods or mechanisms are periodically reviewed and verified.	Yes	No	Don't Know

IT Staff Survey (cont.)			
Practice	**Is this practice used by your organization?**		
Vulnerability Management			
There is a documented set of procedures for managing vulnerabilities, including • selecting vulnerability evaluation tools, checklists, and scripts • keeping up to date with known vulnerability types and attack methods • reviewing sources of information on vulnerability announcements, security alerts, and notices • identifying infrastructure components to be evaluated • scheduling of vulnerability evaluations • interpreting and responding to the results • maintaining secure storage and disposition of vulnerability data	Yes	No	Don't Know
Vulnerability management procedures are followed and are periodically reviewed and updated.	Yes	No	Don't Know
Technology vulnerability assessments are performed on a periodic basis, and vulnerabilities are addressed when they are identified.	Yes	No	Don't Know
Encryption			
Appropriate security controls are used to protect sensitive information while in storage and during transmission (e.g., data encryption, public key infrastructure, virtual private network technology).	Yes	No	Don't Know
Encrypted protocols are used when remotely managing systems, routers, and firewalls.	Yes	No	Don't Know

IT Staff Survey (cont.)	
Practice	**Is this practice used by your organization?**
Security Architecture and Design	
System architecture and design for new and revised systems include considerations for • security strategies, policies, and procedures • history of security compromises • results of security risk assessments	Yes No Don't Know
The organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.	Yes No Don't Know
Incident Management	
Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations.	Yes No Don't Know
Incident management procedures are periodically tested, verified, and updated.	Yes No Don't Know
There are documented policies and procedures for working with law enforcement agencies.	Yes No Don't Know

IT Staff Survey (cont.)			
Practice	**Is this practice used by your organization?**		
General Staff Practices			
Staff members follow good security practice, such as • securing information for which they are responsible • not divulging sensitive information to others (resistance to social engineering) • having adequate ability to use information technology hardware and software • using good password practices • understanding and following security policies and regulations • recognizing and reporting incidents	Yes	No	Don't Know
All staff at all levels of responsibility implement their assigned roles and responsibility for information security.	Yes	No	Don't Know
There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides.	Yes	No	Don't Know

References

[Alberts 01] Alberts, Christopher, and Dorofee, Audrey. *OCTAVE Method Implementation Guide v2.0.* Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001.

[Allen 01] Allen, Julia H. *The CERT Guide to System and Network Security Practices*, New York, NY: Addison Wesley, 2001.

[BSI 95] British Standards Institution. *Information Security Management, Part 1: Code of Practice for Information Security Management of Systems* (BS7799: Part 1 : 1995). London, England: British Standard Institution, February 1995.

[Treasury 01] Department of the Treasury, Federal Reserve System, and Federal Deposit Insurance Corp. "Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness; Proposed Rule." *Federal Register* vol. 65, no. 123 (June 2001): 39471-39489.

[HHS 98] Department of Health and Human Services. "Security Standards and Electronic Signature Standards; Proposed Rule." *Federal Register* vol. 63, no. 155 (August 1998): 43242-43280.

[Swanson 96] Swanson, Marianne, and Guttman, Barbara. *Generally Accepted Principles and Practices for Securing Information Technology Systems* (NIST SP 800-14). Washington, DC: National Institute of Standards and Technology, Department of Commerce, 1996.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	October 2001	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
OCTAVE Catalog of Practices, Version 2.0	F19628-00-C-0003

6. AUTHOR(S)

Christopher J. Alberts, Audrey J. Dorofee, Julia H. Allen

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2001-TR-020

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	ESC-TR-2001-020

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

The Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE℠) Method enables organizations to identify the risks to their most important assets and build mitigation plans to address those risks. OCTAVE uses three "catalogs" of information to maintain modularity and keep the method separate from specific technologies. One of these catalogs is the catalog of good security practices. It provides the means to measure an organization's current security practices and to build a strategy for improving its practices to protect its critical assets.

The catalog of practices is divided into two types of practices – strategic and operational. The strategic practices focus on organizational issues at the policy level and provide good, general management practices. Operational practices focus on the technology-related issues dealing with how people use, interact with, and protect technology. This technical report describes how the catalog of practices is used in OCTAVE and describes the catalog in detail.

14. SUBJECT TERMS	15. NUMBER OF PAGES
assets, information security, risk management, security practices	60

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL